SECRET

FEB 0 3 2017

CERRID # 33143613

MEMORANDUM FOR THE MINISTER OF NATIONAL DEFENCE

Response to CSE Commissioner's

Review of the CSE Procedural Errors and CSE and Second Party Privacy Incidents

(For Approval)

Summary

- The CSE Commissioner completed his annual *Review of the CSE Procedural Errors and CSE and Second Party Privacy Incidents*.
-
-

BACKGROUND

- You received a letter and report from the CSE Commissioner, dated January 6, 2017, providing the results of his *Review of the CSE Procedural Errors and CSE and Second Party Privacy Incidents*.
- The review examined the process that CSE uses to monitor compliance of its operations with legal responsibilities, ministerial requirements, operational policies and procedures. The process involves compliance incidents and procedural errors of privacy interest, and the associated mitigative and corrective actions.
- The review examined three files including CSE Privacy Incident File (PIF), Second Party Incidents File (SPIF) and Minor Procedural Errors Record (MPER). The SPIF was introduced in January 2016 to clarify the record keeping process in relation to incidents attributable to CSE from those attributable to Second Party partners.
-

CONSIDERATIONS

- This review examined incidents recorded in the first six months of 2016, as well as two incidents that remained outstanding from late 2015.
-
-
-

NEXT STEPS

- Enclosed is a package for your consideration and response to the CSE Commissioner.

Greta Bossenmaier
Chief

TOP SECRET//SI//CEO

Our file # 2200–109

January 6, 2017

The Honourable Harjit Sajjan, PC, OMM, MSM, CD, MP
Minister of National Defence
101 Colonel By Drive
Ottawa, ON K1A 0K2

Subject: Review of CSE Procedural Errors and CSE and Second Party Privacy Incidents

Dear Minister:

The purpose of this letter is to provide you with the results of the most recent review of the Communications Security Establishment (CSE) Minor Procedural Errors File (MPEF), Privacy Incidents File (PIF), and new Second Party Incidents File (SPIF), which was implemented on January 1, 2016. The review was undertaken under the Commissioner's general authority articulated in Part V.1, paragraph 273.63(2)(*a*) of the *National Defence Act* (NDA).

Based on the review of the MPEF, PIF and SPIF records, CSE's answers to questions, and an independent verification of information in CSE databases,

Background

CSE policy OPS-1, *Protecting the Privacy of Canadians and Ensuring Legal Compliance in the Conduct of CSEC Activities* (December 1, 2012), requires CSE foreign signals intelligence and information technology security employees to report and document privacy incidents. CSE reports and tracks privacy incidents and procedural errors, and the associated mitigative and corrective actions, as one measure to promote compliance with legal and ministerial requirements and operational policies and procedures, and to enhance the protection of the privacy of Canadians.

CSE examines compliance incidents to determine whether internal or external recipients were exposed to sensitive personal information of Canadians without appropriate authorization, and whether the incidents could result in potential harm to the Canadians. The PIF is a record of incidents attributable to CSE involving activities conducted in a manner counter to CSE operational policy and privacy guidelines and information being exposed to external stakeholders who ought not to have received it. The SPIF is a record of similar compliance incidents attributable to second party partners. These incidents may be identified by the partners themselves, or by CSE. The MPEF is a record of incidents where the information was contained within CSE and not exposed to external recipients.

Treasury Board of Canada Secretariat (TBS) makes a further distinction, defining a material privacy breach as a breach that "involves sensitive personal information and could reasonably be expected to cause serious injury or harm to the individual and/or involves a large number of affected individuals" (*Guidelines for Privacy Breaches*, section 4, May 5, 2014).

During the year, the Commissioner's office examines privacy incidents as part of separate, in-depth reviews of CSE activities, including the associated entries in the PIF and SPIF. However, individual reviews may not capture all incidents and CSE's response might be pending when an individual review report is issued.

The annual review of the MPEF, PIF and, as of this year, SPIF, focuses on incidents not examined in detail in the course of other reviews. It permits the identification of trends or systemic weaknesses that might suggest a need for corrective action, changes to CSE's procedures or policies, or an in-depth review of a specific incident or activity. For example, the office could investigate an incident identified by CSE as a material privacy breach or could examine an incident to determine whether it was a material privacy breach.

The objectives of the review were to:

- acquire knowledge of the procedural errors, incidents and subsequent actions taken by CSE to correct the incidents or mitigate the consequences;
- acquire knowledge of any CSE operational material privacy breaches and CSE's associated corrective actions;
- determine what incidents, if any, may raise questions about compliance with the law or the protection of the privacy of Canadians; and
- help evaluate CSE's policy compliance validation framework and monitoring activities.

Methodology

The review is based on an examination of the MPEF, PIF and SPIF records for the period, CSE's answers to questions, and an independent verification by the office of reports in — which is CSE's database of end-product reports — as well as Canadian entities designated as Protected in which is CSE's target information database.

Findings

MPEF

in the MPEF noted a discovery that an analyst's account folder, which was linked to a "raw" (i.e., unassessed) data repository, contained files dating from that may have contained private communications and that had not been deleted in accordance with CSE's retention schedule. According to CSE, the folder was subsequently deleted without any of its files having been opened, and CSE undertook to routinely review and delete the data in that repository.

other entries involved Canadian Identity Information (CII) being made available to one or more unintended recipients within CSE due to technical issues and/or human error; technical solutions were implemented to prevent reoccurrences. involved having potential unintended access to however, according to CSE officials, access logs confirmed that only authorized persons actually viewed the data. consisted of the inadvertent inclusion of a Canadian identity in an end-product report; however, based on CSE information, audit logs confirmed that only CSE employees — specifically the report's two authors and two CSE Client Relations Officers — had accessed the report before it was cancelled.

PIF and SPIF

A total of 55 privacy incidents were reported in the six-month period under review — attributable to CSE (PIF) and to its second party partners (SPIF).

Of the incidents attributable to CSE, involved the inadvertent sharing or inclusion in a report of CII without suppressing the information in accordance with CSE naming policies. In all but one of these incidents, it was unknown at the time the reports were issued that the information pertained to a Canadian or a person in Canada. The remaining incident was due to human error and was quickly rectified. In all instances, the reports were cancelled or corrected with the identities properly suppressed. In incidents, the nationality of the Canadian was known within certain areas of CSE, that is, specifically

incidents also involved the sharing within CSE of CII obtained from reporting that should have had a very limited distribution within CSE given the sensitivity of the information.

The remaining incidents involved unintentional targeting or database searches for information relating to individuals not previously known to be Canadian or persons in Canada. In several of these incidents, the incidents involved a foreign intelligence target One instance involved a targeting incident in support to a request for assistance from under part (c) of CSE's mandate, before receiving all required authorizations from CSE senior management. In all of these instances, CSE deleted any associated intercepted communications or reporting.

Of the privacy incidents attributable to the Second Parties, involved the inclusion in a report of CII of individuals not previously known to be Canadian or persons in Canada. Another incident involved a report that mistakenly labelled a Canadian as a national of a second party country. While the Canadian was not identified in the report, it is uncertain whether, as a consequence of the mislabeling, the Canadian's identity might have been subsequently shared by second party partners with their clients without the express permission of CSE. The final incident consisted of a Canadian permanent resident having been named in a total of reports issued by second party partners during the period. In when CSE authorities became aware that these reports existed, a report cancellation request was issued to agencies; however, owing to the age of the reports, the report cancellations, which were carried out by the originating agencies, did not automatically result in the reports being deleted from as they normally would. When it was discovered, months later, that the reports still resided in CSE manually purged them from the system.

As part of the review, office employees reviewed end-product reports in that were referenced in the SPIF. They discovered that of the second party reports contained an belonging to a Canadian, even though both reports had been reissued with the CII suppressed and CSE had received confirmation by the issuing second party partner that the original reports had been cancelled. As a follow-up to the office's inquiry, CSE manually purged these reports from It is not clear why the reports had not been deleted from automatically upon their cancellation, as expected.

The Deputy Chief, Policy and Communications, is CSE's Chief Privacy Officer, and is responsible for determining, in consultation with the Department of Justice Canada, if an incident constitutes a material privacy breach. Such determination is guided by the TBS diagnostic tools relating to material privacy breaches and CSE's internal policies and procedures. CSE did not identify any operational material privacy breach as having occurred during the period under review.

General observations and opportunities to enhance privacy protection

Since the previous review, CSE issued PCI-4, *Handling Operational Compliance Incidents*, a new policy instrument setting out the procedures for CSE employees to follow in handling privacy incidents and procedural errors. CSE quickly corrected minor inconsistencies in the policy identified by the office.

Before this letter was finalized, CSE officials had an opportunity to review it for factual accuracy and to comment on the findings.

If you have any questions or comments, I will be pleased to discuss them with you at your convenience.

Yours sincerely,

Jean-Pierre Plouffe

cc: Ms. Greta Bossenmaier, Chief, CSE

Minister of National Defence

Ministre de la Défense nationale

Ottawa, Canada K1A 0K2

SECRET

CERRID # 33183524

FEV FEB 21 2017

The Honourable Jean-Pierre Plouffe
Communications Security Establishment Commissioner
90 Sparks Street, Suite 730
P.O. Box 1984, Station B
Ottawa, Ontario, K1P 5B4

Dear Commissioner Plouffe:

I am writing to respond to your report dated 6 January 2017, entitled *Review of the CSE Procedural Errors and CSE and Second Party Privacy Incidents*.

Thank you for advising me of the results of this review.

Sincerely,

The Hon. Harjit S. Sajjan, PC, OMM, MSM, CD, MP

cc: Greta Bossenmaier, Chief, CSE

Canada

Department of Justice Canada / Ministère de la Justice Canada

Security classification -- Côte de sécurité
Solicitor Client Privilege Top Secret
File number -- Numéro de dossier
50000-02
Date
January 24, 2017
Telephone / FAX -- Téléphone / Télécopieur
(613) 991-8393 -- (613) 991-7379

MEMORANDUM – NOTE DE SERVICE

TO / DEST: Greta Bossenmaier Chief, CSE

FROM / ORIG: Christine Evans, Counsel, Legal Services, Communications Security Establishment

SUBJECT / OBJET:

Do not write in this space / Ne pas écrire dans cet espace

Christine Evans
Counsel

cc: Dominic Rochon, DCPC
Shelly Bruce, DCSIGINT
Scott Jones, DCITS